IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Huayan Wang Bruce A. Willins	Group Art Unit:	2152
		Examiner:	Chad Zhong
Serial No.:	10/029,772	Atty. Dkt. No.:	6000.001900
Filed:	December 21, 2001	Client Docket:	1273
For:	Mail Security Method And System	Confirmation #:	4705

CORRECTED APPEAL BRIEF

Customer No.: 23720

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants hereby submit this Corrected Appeal Brief to the Board of Patent Appeals and Interferences in response to the Notification of Non-Compliant Appeal Brief dated August 16, 2006. The Notice of Appeal was filed on March 2, 2006.

The fee for filing this Appeal Brief is $500, and has already been paid.

Should any additional fees under 37 C.F.R. §§ 1.16 to 1.21 be required for any reason relating to the enclosed material, or should an overpayment be included herein, the Commissioner is authorized to deduct or credit said fees from or to Williams, Morgan & Amerson, P.C. Deposit Account No. 50-0786/6000.001900.

I. REAL PARTY IN INTEREST

The present application is owned by Symbol Technologies, Inc..

II. RELATED APPEALS AND INTERFERENCES

Applicants are not aware of any related appeals and/or interferences that might affect the outcome of this proceeding.

III. STATUS OF THE CLAIMS

Claims 1-28 are pending in the application. Claims 1-28 are at issue in this appeal and they are attached as Appendix A. Claims 1-7 and 10-15 were rejected in the Final Office Action issued on November 2, 2005 as allegedly being unpatentable under 35 U.S.C. § 103(a) over U. S. Patent 6,260,029 ("***Critelli***") in view of U.S. Patent Application Publication 2002/0013899 ("***Faul***"). Claims 8 and 9 were rejected as allegedly being unpatentable under 35 U.S.C. § 103(a) over ***Critelli*** in view of ***Faul*** and further in view of Applicant Admitted Prior Art (hereafter, AAPA). Claims 18-21 and 23-28 were rejected as allegedly being unpatentable under 35 U.S.C. § 103(a) over ***Critelli*** in view of ***Faul*** and further in view of U. S. Patent 5, 917, 925 ("***Moore***"). All the pending claims 1-28 are the subject of the present appeal.

IV. STATUS OF AMENDMENTS

No amendments have been filed subsequent to the Final Office Action.

V. SUMMARY OF CLAIMED SUBJECT MATTER

In general, the present invention is directed to a security envelope with a barcode carrying a digital signature signed by the sender. For example, the sender may be the first mailman at the entrance point of the postal system. Such a system may impose non-repudiation on the sender at its location or at its drop-off point. To provide authentication information, the barcode may be scanned and tracked at each point from the source to the destination. There are three independent claims at issue in the current appeal: claims 1, 10 and 23.

Independent claim 1 is generally directed to a security envelope. The security envelope comprises a barcode in a two-dimensional symbology located on the security envelope. The barcode encodes a public component comprising a digital signature signed by the sender encrypted by the private key of the sender and a private component comprising a digital signature signed by the sender encrypted by the public key of the receiver. By way of example only, at least portions of the invention are described at p. 2-11; Figures 1, 3 and 4.

Independent claim 10 is generally directed to a method for securing the mails. The method comprises producing a digital mail identification that encodes physical identification information of a security envelope into a barcode in a two-dimensional symbology. The digital mail identification comprises: (a) a public component, the public component comprising a public digital mail identification and a digital signature signed by the sender encrypted by the private key of the sender; and (b) a private component, the private component comprising a digital mail identification and a digital signature signed by the sender encrypted by the public key of the receiver. The method further comprises applying the digital mail identification to the security envelope. By way of example only, at least portions of the invention are described at p. 2-11; Figures 1, 3 and 4.

Independent claim 23 is generally directed to a system of securing the mails. The system comprises at least one security envelope, comprising (a) a barcode in a two-dimensional symbology located on the security envelope. The barcode encodes (i) a public component, the public component comprising a public digital mail identification and a digital signature signed by the sender encrypted by the private key of the sender; and (ii) a private component, the private component comprising a digital mail identification and a digital signature signed by the sender

encrypted by the public key of the receiver. The system further comprises at least one mobile computer, comprising: a bar code reader; a physical authentication identifier reader; computer capable of comparing information obtained from the bar code reader and the physical authentication identifier reader; a database capable of storing at least one public key and at least one private key; a display; and a printer. By way of example only, at least portions of the invention are described at p. 2-11; Figures 1, 3 and 4.

Dependent claim 3 is generally directed to a security envelope. In the security envelope, the barcode further encodes return address information. By way of example only, at least portions of the invention are described at p. 2-11; Figures 1, 3, and 4.

Dependent claim 8 is generally directed to a security envelope. In the security envelope, the physical authentication identification comprises an optically clear epoxy with air bubbles suspended therein. By way of example only, at least portions of the invention are described at p. 2-11; Figures 1, 3, and 4.

Dependent claim 9 is generally directed to a security envelope. In the security envelope, the physical authentication identification comprises a cloth made from non-woven 40 micron diameter polymer fibers. By way of example only, at least portions of the invention are described at p. 2-11; Figures 1, 3, and 4.

Dependent claim 12 is generally directed to a method for securing the mails. In the method, the physical identification information comprises return address information. By way of example only, at least portions of the invention are described at p. 2-11; Figures 1, 3, and 4.

Dependent claim 18 is generally directed to a method for securing the mails. The method

further comprises measuring the physical identification information, decoding the digital mail identification, and comparing the measured physical identification information with the decoded digital mail identification. By way of example only, at least portions of the invention are described at p. 2-11; Figures 1, 3, and 4.

Dependent claim 19 is generally directed to a method for securing the mails. The method further comprises at least one of the steps of (1) measuring the physical identification information, and (2) decoding the digital mail identification is accomplished using an optical scanner. By way of example only, at least portions of the invention are described at p. 2-11; Figures 1, 3, and 4.

Dependent claim 20 is generally directed to a method for securing the mails. The method further comprises the step of comparing the measured physical identification information with the decoded digital mail identification is accomplished using a mobile computer. By way of example only, at least portions of the invention are described at p. 2-11; Figures 1, 3, and 4.

Dependent claim 21 is generally directed to a method for securing the mails. The method further comprises transmitting the measured physical identification information and the decoded digital mail identification to a wired computer network via a wireless medium. By way of example only, at least portions of the invention are described at p. 2-11; Figures 1, 3, and 4.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Appellants respectfully request that the Board review and overturn the three rejections present in this case. The following issues are presented on appeal in this case:

(A) Whether claims 1-7 and 10-15 are obvious over ***Critelli*** in view of ***Faul***?

(B) Whether claims 8, 9 and 16, 17 are obvious over ***Critelli*** in view of ***Faul*** and further in view of Applicant Admitted Prior Art (hereafter, AAPA) ?

(C) Whether claims 18-21 and 23-28 are obvious over ***Critelli*** in view of ***Faul*** and further in view of ***Moore*** ?

(D) Whether claims 3 and 12 are obvious over ***Critelli*** in view of ***Faul*** ?

VII. ARGUMENT

Applicants respectfully submit that the Examiner erred in rejecting claims 1-28 for reasons fully set forth below. Therefore, Applicants respectfully request that the rejection of claims 1-7 and 10-15 under 35 U.S.C. §103(a) as allegedly being unpatentable over ***Critelli*** in view of ***Faul,*** claims 8 and 9 under 35 U.S.C. §103(a) as allegedly being unpatentable over ***Critelli*** in view of ***Faul*** and further in view of Applicant Admitted Prior Art (hereafter, AAPA), and claims 18-21 and 23-28 under 35 U.S.C. §103(a) as allegedly being unpatentable over ***Critelli*** in view of ***Faul*** and further in view of ***Moore*** be reversed.

(A) Claims 1-7 and 10-15 are not obvious over *Critelli* in view of *Faul*

1. Legal Standard

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable

expectation of success must both be found in the prior art, and not based on Applicants' disclosure. *In re Vaeck*, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991); M.P.E.P. § 2142. Moreover, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 U.S.P.Q. 580 (CCPA 1974). If an independent claim is nonobvious under 35 U.S.C. § 103, then any claim depending therefrom is nonobvious. *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988); M.P.E.P. § 2143.03.

With respect to alleged obviousness, there must be something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination. *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561 (Fed. Cir. 1986). In fact, the absence of a suggestion to combine is dispositive in an obviousness determination. *Gambro Lundia AB v. Baxter Health-care Corp.*, 110 F.3d 1573 (Fed. Cir. 1997). The mere fact that the prior art can be combined or modified does not make the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990); M.P.E.P. § 2143.01. The consistent criterion for determining obviousness is whether the prior art would have suggested to one of ordinary skill in the art that the process should be carried out and would have a reasonable likelihood of success, viewed in the light of the prior art. Both the suggestion and the expectation of success must be founded in the prior art, not in the Applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991; *In re O'Farrell*, 853 F.2d 894 (Fed. Cir. 1988); M.P.E.P. § 2142.

Federal Circuit precedent makes it crystal clear that, in an obviousness situation, the prior art must disclose each and every element of the claimed invention, and that any motivation to combine or modify the prior art must be based upon a suggestion in the prior art. *In re Lee*, 61 U.S.P.Q.2d 143 (Fed. Cir. 2002). Conclusory statements regarding common knowledge and

common sense are insufficient to support a finding of obviousness. *Id.* at 1434-35. Thus, to establish a *prima facie* case of obviousness, the prior art reference (or references when combined) must teach or suggest all the claim features. Additionally, the references must provide a motivation to combine in the manner suggested by the Examiner. Mere conclusory statements to combine are insufficient.

2. The Cited References Do Not Teach Each and Every Claim Feature

In the Final Office Action mailed on November 2, 2005, the Examiner has maintained the rejection of claims 1-7 and 10-15 under 35 U.S.C. § 103(a) over ***Critelli*** in view of ***Faul***. Applicants respectfully traverse the Examiner's rejection

Claim 1 is directed to a security envelop. The security envelop comprises a barcode in a two-dimensional symbology located on the security envelope. The barcode encodes a public component and a private component. The public component comprises a digital signature signed by the sender encrypted by the private key of the sender. The private component comprises a (1) digital signature signed by the sender and (2) encrypted by the public key of the receiver.

The Examiner alleges that ***Critelli*** and ***Faul***, in combination, teach all the elements of claim 1. The Applicants respectfully disagree and assert that neither ***Critelli*** nor ***Faul*** at least teaches or suggests a private component that comprises (1) a digital signature signed by the sender and (2) encrypted by the public key of the receiver.

The Examiner argues that the "public component" of claim 1 corresponds to the bar code 36 (including "shipping" and "postal verification" information) in ***Critelli***, and the "private component" corresponds to the "non-shipping" and "advertising" information disclosed in

Critelli. *See* Final Office Action, p. 2. The Examiner further alleges that ***Critelli*** discloses that the "non-shipping" information is signed by the sender. *See*, the Final Office Action (p. 2) and the Advisory Office Action (p. 2). This is plainly incorrect. A closer review of ***Critelli*** reveals that the non-shipping information ("private component" according to the Examiner) is, in fact, digitally signed by a third party, and not the sender, as called for by claim 1. See ***Critelli,*** Col. 4, lines 10-15 (stating bar code 37 includes information signed by the third party). In fact, the Examiner concedes that the non-shipping information is not signed by the sender, but rather a third party. *See* Advisory Action, p. 2. The other references cited by the Examiner also do not teach the claimed feature of a private component comprising a digital signature that is signed by the sender. Thus for this reason alone, claims 1-7 and 10-15 are allowable.

The cited references also do not teach or suggest a private component encrypted by the public key of the receiver. The Examiner admits that ***Critelli*** does not teach the feature of encrypting the private component using the public key of the receiver. To remedy at least the acknowledged deficiencies of the primary reference, the Examiner relies on ***Faul***. However, as explained below, the Examiner's reliance on ***Faul*** is misplaced because not only has the Examiner failed to provide the requisite motivation to combine the references in the manner suggested, but the Examiner has also failed to recognize that ***Faul*** teaches against the proposed combination.

As an initial matter, the Examiner's reliance on ***Faul*** for the obviousness rejection is problematic because ***Faul*** is unrelated to the Applicants' field of invention. ***Faul*** is directed transmitting stock-related information between a sender and a receiver. *See* ***Faul,*** paragraph [0008]. In contrast, the present invention is directed to bar codes. The Examiner thus runs afoul

of the well-established principle that a 103 reference must be within Applicant's field of endeavor. *In re Clay*, 23 U.S.P.Q.2d (BNA) 1058, 1060 (Fed. Cir. 1992)

Aside from relying on a reference unrelated to Applicants' field of endeavor, the Examiner's obviousness rejection is erroneous because ***Faul*** teaches away from the claimed combination. In applying ***Faul***, the Examiner asserts that the "essential elements" of a transaction disclosed in ***Faul*** correspond to the "public component" of the claims. *See* Final Office Action, p. 3. ***Faul***, however, explains that this so-called "essential elements" are, in fact, encrypted with the public key of the receiver. *See* ***Faul,*** paragraph [0029] (describing that essential elements 404 encrypted using the vendee's (receiver) public key). In contrast, the claims call for encrypting the public component using the private key of the sender. Moreover, ***Faul*** is inconsistent with the teachings of ***Critelli***, which describes encrypting "shipping information" (the "public component" per the Examiner) using the private key of the sender. On the other hand, as noted, Faul teaches signing the "essential elements" ("public component) according to the Examiner) with receiver's public key. Thus, not only does ***Faul*** not provide the requisite motivation to combine the references in the manner suggested, it actually teaches away from such a combination. For this additional reason, the Examiner's obviousness rejection is flawed.

3. The Examiner's Response

Responding to the Applicants' contention that ***Critelli*** does not teach a private component comprising a digital signature that is signed by the sender, the Examiner argued in the Advisory Action that such a feature is taught at col. 4, lines 13-14 of ***Cirtelli***. *See* Advisory Action. The cited passage states "bar code 36 on the other hand includes postal verification

information signed by the sender." As can be seen, this passage is referring to bar code 36, which the Examiner has acknowledged (on page 2 of the Final Office Action) corresponds to the "public" component, not the "private" component, of the claimed invention. The Examiner further acknowledged in the Final Office Action that the "postal verification information" and "shipping information" are part of the bar code 36. Thus, contrary to the Examiner's assertion, the passage cited at col. 14 does not teach a private component comprising a digital signature that is signed by the sender.

(B) Claims 8 and 9 are not obvious over *Critelli* in view of *Faul* and further in view of Applicant Admitted Prior Art (hereafter, AAPA)

Claims 8 and 9 are dependent claims of independent claim 1. Claim 8 sets forth, in addition to the features specified in the independent claim and any intervening claims, that the physical authentication identification comprises an optically clear epoxy with air bubbles suspended therein. Here, the Examiner simply refers to the Applicants' patent application and alleges that the recited feature of clam 8 was known in the prior art. The Examiner then provides a conclusory statement for motivation to combine the Applicants' disclosure with the teachings of ***Critelli*** and ***Faul***. The Examiner does not point to a single reference in the prior art reference for the alleged motivation. Thus, the Examiner's conclusory statement is legally deficient. It is well-established under Federal Circuit's precedent that conclusory statements regarding common knowledge and common sense are insufficient to support a finding of obviousness.

(C) Claims 18-21 and 23-28 are not obvious over *Critelli* in view of *Faul* and further in view of *Moore*

Claims 18 is a dependent claim of independent claim 11. Claim 18 sets forth, in addition to the features specified in the independent claim, measuring the physical identification information, decoding the digital mail identification and comparing the measured physical identification information with the decoded digital mail identification. The Examiner relies on ***Moore*** (U.S. Patent No. 5, 917, 925) to reject claim 18-21 and 23-28 under 35 U.S.C. §103(a) to overcome the admitted fundamental deficiencies in ***Critelli*** and ***Faul***. However, ***Moore*** fails to address the above-indicated shortcomings of ***Critelli*** and ***Faul***.

The Examiner argues that the features recited in claim 18 are disclosed in ***Moore*** at col. 4, lines 35-45. However, the cited passage at least does not teach or suggest measuring the physical identification information. Instead, the cited passage ***describes*** decoding a mark and comparing it to marks pre-stored in a computer. The Examiner asserts that the pre-stored marks are "measuring the physical identification information" of the claims. But storing pre-stored marks is not "measuring." Rather, it is simply storing marks in a storage unit. Accordingly, notwithstanding the Examiner's assertion, ***Moore*** does not teach or suggest measuring the physical identification information. Therefore, the ***Moore*** reference fails to remedy the fundamental deficiencies of ***Critelli*** and ***Faul.***

The Applicants also assert that the Examiner has failed to establish the requisite motivation to combine the references in the manner suggested. The Examiner provides a conclusory statement without any support in the cited reference themselves to establish a motivation to combine. This is clearly inadequate. For this additional reason, the claims are allowable.

For reasons presented above, Applicants respectfully submit that the Examiner has failed to make a *prima facie* case that claims 18 and 23 are obvious over ***Critelli*** in view of ***Faul*** and further in view of ***Moore***.

(D) Claims 3 and 12 are not obvious over *Critelli* in view of *Faul*

Claims 3 and 12 are allowable over the cited references for at least the reasons their respective independent claims 1 and 12 are allowable. Moreover, these claims are also allowable for the additional features recited therein. In particular, claims 3 and 12 specify the barcode further encodes return address information. This feature is not disclosed in ***Critelli*** or ***Faul***.

The Examiner asserts that ***Critelli*** in Col. 2, lines 35-50 teaches or suggests a barcode that encodes return address information. To the contrary, the cited passage simply describes that the mail package (i.e., sealed package 11) contains the sender's address field 13. This passage does not describe that the barcode itself is encoded with the return address information. In fact, ***Critelli*** clarifies that the bar code 36 does not include encoded return address information but rather includes information relating to the recipient's address field. See ***Critelli,*** Col. 2, lines 45-46 (stating that the barcode 36 includes cryptographically secured information derived only from the address field 12). Like ***Critelli***, ***Faul*** also fails to supply this missing claimed feature. Thus, claims 3 and 12 are allowable for this additional reason.

The Applicants also assert that the Examiner has failed to establish the requisite motivation to combine the references in the manner suggested. The Examiner provides absolutely no motivation to combine the references in the manner suggested in rejecting claims 3 and 12. For this additional reason, these claims are allowable.

VIII. CLAIMS APPENDIX

The claims that are the subject of the present appeal – claims 1-28 – are set forth in the attached "Claims Appendix."

IX. EVIDENCE APPENDIX

Applicants do not rely upon any evidence as indicated on the attached Evidence Appendix.

X. RELATED PROCEEDINGS APPENDIX

There are no Related Proceedings for this appeal as indicated on the attached Related Proceedings Appendix.

XI. CONCLUSION

Accordingly, it is respectfully submitted that the Examiner erred in not allowing claims 1-28 over the prior art of record. Applicants respectfully request the Board reverse the Examiner's rejections. The undersigned agent may be contacted at (713) 934-4089 with respect to any questions, comments or suggestions relating to this appeal.

Respectfully submitted,
WILLIAMS, MORGAN & AMERSON

/Sanjeev K. Singh, Ph.D./

Date: September 5, 2006

Sanjeev K. Singh, Ph.D
Reg. No. L0220
10333 Richmond Ave., Suite 1100
Houston, Texas 77042
(713) 934-4089 ph
(713) 934-7011 fx
AGENT FOR APPLICANTS

CLAIMS APPENDIX

1. (Previously Presented) A security envelope, comprising:

a barcode in a two-dimensional symbology located on the security envelope, the barcode encoding:

a public component comprising a digital signature signed by the sender encrypted by the private key of the sender;

and

a private component comprising a digital signature signed by the sender encrypted by the public key of the receiver.

2. (Previously Presented) The security envelope as in claim 1, wherein the public component and the private component each include a digital mail identification.

3. (Original) The security envelope as in claim 2, wherein the barcode further encodes return address information.

4. (Original) The security envelope as in claim 2, wherein the barcode further encodes information relating to the physical characteristics of the security envelope.

5. (Original) The security envelope as in claim 4, wherein the information relating to the physical characteristics of the security envelope include at least one of: (a) the date the security envelope was sealed; (b) the size of the security envelope; and (c) the weight of the security envelope.

6. (Original) The security envelope as in claim 2, wherein the barcode further encodes stamp information.

7. (Original) The security envelope as in claim 2, wherein the security envelope further comprises a physical authentication identification and wherein the barcode further comprises a digital representation of the physical authentication identification.

8. (Original) The security envelope as in claim 7, where the physical authentication identification comprises an optically clear epoxy with air bubbles suspended therein.

9. (Original) The security envelope as in claim 7, where the physical authentication identification comprises a cloth made from non-woven 40 micron diameter polymer fibers.

10. (Previously Presented) A method for securing the mails, comprising:

(1) producing a digital mail identification that encodes physical identification information of a security envelope into a barcode in a two-dimensional symbology; wherein the digital mail identification comprises:

(a) a public component, the public component comprising a public digital mail identification and a digital signature signed by the sender encrypted by the private key of the sender;

and

(b) a private component, the private component comprising a digital mail identification and a digital signature signed by the sender encrypted by the public key of

the receiver;

(2) applying the digital mail identification to the security envelope.

11. (Original) The method as in claim 10, where the two-dimensional symbology is PDF -417.

12. (Original) The method as in claim 11, wherein the physical identification information comprises return address information.

13. (Original) The method as in claim 11, wherein the physical identification information comprises information relating to the physical characteristics of the security envelope.

14. (Original) The method as in claim 13, wherein the information relating to the physical characteristics of the security envelope include at least one of:

(a) the date the security envelope was sealed;

(b) the size of the security envelope; and

(c) the weight of the security envelope.

15. (Original) The method as in claim 11, wherein the physical identification information comprises stamp information.

16. (Original) The method as in claim 11, where the physical identification information comprises an optically clear epoxy with air bubbles suspended therein.

17. (Original) The method as in claim 11, where the physical identification information comprises a cloth made from non-woven 40 micron diameter polymer fibers.

18. (Previously Presented) The method as in claim 11, further comprising:

measuring the physical identification information;

decoding the digital mail identification; and

comparing the measured physical identification information with the decoded digital mail identification.

19. (Original) The method as in claim 18, wherein at least one of the steps of (1) measuring the physical identification information, and (2) decoding the digital mail identification is accomplished using an optical scanner.

20. (Original) The method as in claim 19, wherein the step of comparing the measured physical identification information with the decoded digital mail identification is accomplished using a mobile computer.

21. (Original) The method as in claim 19, further comprising:

transmitting the measured physical identification information and the decoded digital mail identification to a wired computer network via a wireless medium.

22. (Original) The method as in claim 21, wherein the wired computer network is connected to the Internet and the transmitting the identification data to a wired computer network via a wireless medium uses a TCP/IP protocol.

23. (Previously Presented) A system of securing the mails, comprising:

(1) at least one security envelope, comprising

(a) a barcode in a two-dimensional symbology located on the security envelope, the barcode encoding:

(i) a public component, the public component comprising a public digital mail identification and a digital signature signed by the sender encrypted by the private key of the sender; and

(ii) a private component, the private component comprising a digital mail identification and a digital signature signed by the sender encrypted by the public key of the receiver;

(2) at least one mobile computer, comprising:

(a) a bar code reader;

(b) a physical authentication identifier reader;

(c) computer capable of comparing information obtained from the bar code reader and the physical authentication identifier reader;

(d) a database capable of storing at least one public key and at least one private key;

(e) a display; and

(f) a printer.

24. (Original) The system as in claim 23, where the two-dimensional symbology is PDF-417.

25. (Original) The system as in claim 24, where the at least one security envelope further comprises an optically clear epoxy with air bubbles suspended therein.

26. (Original) The system as in claim 24, where the at least one security envelope further comprises a cloth made from non-woven 40 micron diameter polymer fibers.

27. (Original) The system as in claim 24, further comprising:

a wired computer network capable of communication with the at least one mobile computers via a wireless medium.

28. (Original) The system as in claim 27, wherein the wired computer network is connected to the Internet using a TCIP/IP protocol.

BEFORE THE OFFICE OF ENROLLMENT AND DISCIPLINE
UNITED STATES PATENT AND TRADEMARK OFFICE

LIMITED RECOGNITION UNDER 37 CFR § 11.9(b)

Dr. Sanjeev Kumar Singh is hereby given limited recognition under 37 CFR §11.9(b) as an employee of Williams, Morgan & Amerson, P.C., to prepare and prosecute patent applications for clients of Williams, Morgan & Amerson, P.C. in which a member of Williams, Morgan & Amerson, P.C., is the attorney of record. This limited recognition shall expire on the date appearing below, or when whichever of the following events first occurs prior to the date appearing below: (i) Dr. Sanjeev Kumar Singh ceases to lawfully reside in the United States, (ii) Dr. Sanjeev Kumar Singh's employment with Williams, Morgan & Amerson, P.C. ceases or is terminated, or (iii) Dr. Sanjeev Kumar Singh ceases to remain or reside in the United States on an H-1B visa.

This document constitutes proof of such recognition. The original of this document is on file in the Office of Enrollment and Discipline of the U.S. Patent and Trademark Office.

Limited Recognition No. **L0220**
Expires: April 14, 2007

Harry I. Moatz
Director of Enrollment and Discipline